Audit Committee minutes
Monday 18 September 2017

Members:

Ailsa Beaton (chair)	Non-Executive Director
Roger Barlow	Independent Audit Committee member
Jane McCall	Non-Executive Director

Attendees:

<u>ICO</u>	
Paul Arnold	Deputy CEO
Louise Byers	Head of Risk and Governance
Elizabeth Denham	Information Commissioner
Heather Dove	Head of Finance
<u>Internal Auditors</u>	
Phil Keown	Grant Thornton
Paul Eckersley	Grant Thornton
<u>External Auditors</u>	
David Eagles	BDO (by telephone)
<u>Secretariat</u>	
Peter Bloomfield	Senior Corporate Governance Manager

1. Introductions and apologies

1.1. There were apologies from Paul Keane at the NAO.

2. Declaration of interests

2.1. There were no declarations of interest.

3. Matters arising from the previous meeting

3.1. There were no comments on the minutes. Outstanding actions were updated.

4. Commissioner's update

4.1. Elizabeth Denham commented on work ongoing at the ICO, in particular that arising from monitoring the passage of the Data Protection Bill currently before Parliament.

4.2. The Committee was advised that the lease had been signed for additional office space in Wilmslow which would provide capacity for an extra 100 desks.

5. Risk and opportunity register

5.1. Louise Byers was welcomed to the Committee as Head of Risk and Governance. Louise explained the remit of her new role.

5.2. The risk and opportunity register was considered. Louise Byers explained that the register was more comprehensive than previously and was being used in decision making across the ICO. She also noted that risk management was more embedded than it had been.

5.3. Risk appetite in the area of information governance was discussed. The ICO's appetite in this area is minimalist, reflecting the fact that the ICO is willing to take risks in this area so long as they are carefully considered.

5.4. The scoring of the risk that the ICO was not able to spot emerging technological issues was questioned. Paul Arnold explained that this was a policy related risk rather than one linked to the capacity of staff.

Louise Byers to review the wording of the risk (10) to ensure its meaning was clear by the 30 September.

5.5. The scoring of the risk relating to industrial relations was also questioned. Louise Byers advised that the risk wording was being revised.

5.6. Grant Thornton asked whether the risk status shown was net or gross of mitigation. They considered that this

needed to be made clear in the register and that setting a risk status before and after mitigation was helpful in considering mitigating actions.

5.7. Louise Byers explained that the risk was net and added that adding additional complexity to the register was not thought helpful at this moment.

David Eagles to provide Louise Byers with a copy of relevant guidance on risk by 30 September.

5.8. The Committee agreed to the risk register being published with redactions where necessary.

6. Finance

6.1. Heather Dove introduced the finance report. Given the amount of change in the office both budget and expenditure were being carefully monitored.

6.2. The Committee asked about the level of project management expertise in the office, and how well project expenditure was managed. Heather Dove explained that whilst profiling project expenditure was difficult, in general overall expenditure on projects was estimated accurately.

6.3. Audit Committee asked for information detailing whether the ICO was recruiting to profile. Paul Arnold advised that recruitment was on track but there were concerns that not all vacancies would be filled.

6.4. In respect of the 2017/18 accounts and the treatment of additional income from DCMS during the year to cover GDPR implementation costs, the ICO had been in discussion with the NAO and BDO. Heather Dove was working on a technical paper on the matter.

Heather Dove to copy the technical paper to Committee members by 31 October 2017.

7. Outstanding audit recommendations

7.1. It was confirmed that the external audit recommendation relating to payment control weaknesses had been cleared. The control in place was permanent.

7.2. In respect of outstanding actions relating to access to the ICO finance system password it was explained that access could only be given with the authorisation of either Heather Dove or Louise Byers. The actions were therefore considered closed.

7.3. It was agreed to extend the deadline on the action to consider BS 10008.

8. Internal audit

8.1. Grant Thornton advised that the GDPR project review had been finalised. It was confirmed that the review's recommendations had been cleared.

8.2. Grant Thornton provided an update on the internal audit plan for 2017/18.

9. Fraud, whistleblowing and security

9.1. The quarterly report on fraud, whistleblowing and security incidents in Q2 was presented.

9.2. Staff rules on the leaving of ICO resources in cars was questioned and explained.

10. Review of fraud and whistleblowing policies and the Code of Conduct

10.1. Fraud and whistleblowing policies, and the Staff Code of Conduct, were presented to the Committee for review. The Committee received regular reports in issues arising from the policies and the Code and it was thought useful to bring the policies and Code to the Committee on an annual basis for any comments.

10.2. It was agreed to provide the email address of the Audit Committee chair in the documents rather than advising people to ask Corporate Governance to pass on any complaint.

10.3. It was noted that whilst there was a register of staff political interests there was no overarching register of interests for staff other than the most senior. This was questioned.

10.4. The Committee was advised that such a register had been considered but that given the breadth of the ICO regulatory role (across all data controllers in the UK) the effective management of such a register was considered too difficult. Instead the ICO relied upon the Staff Code of Conduct.

10.5. Ways of promoting the Code and other related policies were suggested including promoting the documents regularly

on the intranet and asking staff annually to confirm they had read and understood the documents.

Corporate Governance to take forward suggestions made as to how best to promote the Code and other policies and to report back to the next Audit Committee on what had been done.

11. Any other urgent business

11.1. Ailsa Beaton presented the NAO Round-up for Audit Committees which had been published just before the meeting. It was agreed that the executive would consider matters raised in the document and report back to the next Audit Committee. The need to report on cyber-security issues (mentioned in the round-up) would be linked to the paper on ISO 27001 which was coming to the next Management Board meeting but should also come to the February Audit Committee.

Peter Bloomfield to review the round-up and ensure a report came to the February meeting.

11.2. Peter Bloomfield advised that the dates for Audit Committee had been revised to fit in better with Management Board dates. However the only date that worked for the January meeting was 1 February. It was agreed to go ahead with this meeting in the absence of the Commissioner.

11.3. Peter Bloomfield would circulate other dates as soon as possible and if there were any problems members and attendees were asked to let Corporate Governance know.